BUDDLE FINDLAY

Cyber security - an HR issue as much as an IT issue

Hamish Kynaston

7 October 2016

When people think of cyber security, they often think about technology solutions. These are just the start however - the human elements are just as critical. Documents or emails can be sent to the wrong address, laptops can be left behind, confidential information can be read openly on a plane and employees can be misled into disclosing information.

Businesses need to see cyber security as everyone's issue and educate employees to ensure they are aware of the risks and their responsibilities.

Social engineering

'Social engineering' is a form of hacking that targets individuals - unkindly referred to as 'wetware' - in the hope that an organisation's security systems and training will fail. Often hackers will use information obtained online or from other sources, so that the approach appears credible.

A 'phisher' might for example send an email to a number of people with a link to a fraudulent website from an account that on a first look appears legitimate. Or the hack might be more targeted – sometimes called 'whaling'. It might involve for instance a fraudulent email, allegedly from the CFO, directing someone in accounts to make a payment. To a busy employee, an email from hamish.kynaston@buddlefindlay.com (correct) appears the same as an email from hamish.kynaston@buddlefinlay.com (incorrect).

Managing the risk

Risk management starts with the right leadership. According to PwC's 'Global Economic Crime Survey 2016: Adjusting the Lens on Economic Crime', only 61% of CEOs are concerned about cyber security and less than half of board members request information about their organisation's state of cyber-readiness. In the same way they might approach financial issues or health and safety, the organisation's leaders need to think about the risks they face, the security measures they have in place, and how the organisation will respond if there is a breach.

Policies are helpful. Employees should know for instance not to share passwords; to lock their PC when they're away; the limits around the use of email, the Internet, social media, WiFi and mobile devices (both work and personal); the rules when handling confidential information; and that monitoring occurs.

Policies of course won't keep you secure by themselves. Employees should be educated. For example:

- Provide examples of actual attempts against the organisation or similar organisations - these hold employees' interest more than a list of dos and don'ts
- Provide extra training for customer service and accounts staff - these employees are more likely to be targeted. If an employee is trained to ask enough questions, the social engineer will likely move on
- Test your employees anonymously and publish the results internally
- Remind your employees of the rules. Policies that live in the bottom drawer are quickly forgotten or disregarded.

The organisation should also have a plan on how to respond if and when security is breached. Above all, don't put cyber security in an 'IT box' - it is an organisation-wide and very much a human issue.

This article was written by Hamish Kynaston for the NBR (October 2016).

Auckland

188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659